



CYBER ATTACKS IN THE POST 9/11 ERA: PERSPECTIVES ON NON-STATE ACTORS AND TRANSNATIONAL ARMED CONFLICTS

Assistant Professor Pritam Ghosh

September 14th, 2014



Abstract:

The 9/11 incident has changed the way as to how the world looks at cyber conflicts in the contemporary era. The paradigmatic shift due to the increased involvement of non-state actors has pushed the international community towards the belief that the substantive laws governing cyber attacks require significant amendments. In the 21st century terrorism is now no longer confined to the real world but has gone into the virtual world as well. This has prompted countries all over the world to agree on the usage of a new term called “Cyber-terrorism which involves terrorist activities on the internet by non-State groups who are not affiliated to any state or government but at the same time follow all the characteristics of an Organized Armed Group (OAG) which is normally found in the real world. It is noteworthy that in the real world armed groups use weapons during conflict whereas on the internet this would translate into use of computers and the internet as a weapon to spread terror. In this context, the author argues that a third category of armed conflict, namely ‘transnational armed conflict’ has emerged and the laws of war as well as those related to it like international and transnational criminal laws need to recognize it and mould themselves accordingly.

In consonance with the above findings, the author proposes the adoption of an additional protocol to the “Fourth Geneva Conventions Relative To The Protection Of Civilians During Time Of War (1949)” which would be applicable specifically to transnational conflicts including crimes like transnational cyber-terrorism. A possible definition of a transnational armed conflict will also be given in due course of the suggestions and recommendations which would be capable of being included in the new protocol.

The advancements in the area of information technology across the globe in the last two decades have transformed this planet into a global village and the entire human race into one big community. Computers, internet, hardware, and software have become as much a part of daily human life and habits as some of the other daily routine activities. Subsequently, just as law regulates every aspect of daily human behaviour so does it regulate the use of information technology through a specific branch known as information technology law’. It is noteworthy that information technology is now being used in various fields of work. One such use is in the conduct of war and armed conflicts known as ‘Cyber Warfare’ or ‘Cyber Conflict’.

It is a universally accepted fact that the use of information technology, especially the internet, can help reduce the enormous amount of costs involved in the use of kinetic weapons systems which require appropriate logistics and infrastructural support for application during war. defence departments and ministries around the world subscribe to the view that cyber warfare has many advantages including reducing the risk of unwanted and unintentional collateral physical damage and destruction. At the same time, it can help in striking at the heart of major enemy defence systems, thereby completely incapacitating them and reducing their ability to sustain themselves in war for long periods. In this context, it will be well-placed to discuss the basic idea behind cyber warfare.

Military planners, advisers and thinkers around the world have coined a new term (i.e., “Information Operations (IO)” or “Computer Network Operations (CNO)”) as IO focuses mainly on the use of computer networks as tools and targets of any military operations according to Schmitt in his article; Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. CNO consists of three kinds of manipulative use of computer systems and networks:

(i) *Computer Network Attack* (CNA) which aims to cause severe damage to computer networks and through them; tries to inflict indirect damage on critical national infrastructures.

(ii) *Computer Network Defence* (CND) which is used to protect computer networks from being subjected to damage and destruction, thereby becoming a soft target assailable by enemy networks.

(iii) *Computer Network Exploitation* (CNE) which refers to one-off incidents of manipulation and destruction of data stored in computer networks, hard drives, external devices, and other accessories for mere personal gains or amusement.

The first and third categories represent the offensive elements of IO and the second category represents the defensive category.

It needs to be mentioned here that Computer Network Attack (CNA), also known as “Cyber Attacks” will be the main focus of this paper because compared to CND and CNE it raises complex legal issues regarding the regulation, use, misuse and the methods of use of computer networks in military operations. CNA is defined by the US Department of Defence (Kodar 2012) as; ‘*Actions taken through the use of Computer Networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and the networks themselves*’. In other words, CNA involves the use of computer networks as both tools and targets of large-scale attacks that may eat deep into the defence infrastructures of a country and demonstrate physical damage to both person and property. However, the question is how CNA be differentiated from ordinary cybercrimes (ordinary computer network exploitation) when both use a computer network as a tool and target of attack?

The major differences are firstly; Ordinary Cybercrimes (CNE, as mentioned earlier) are mostly committed by private individuals for their personal gains and are directed against domestic computers whereas CNA commonly involves offensive operations against state defence networks accompanied by visible kinetic warfare. Secondly, CNA has a much greater and sometimes irreparable damaging effect as it aims at the military defence networks of a country often disabling Critical National Infrastructures such as air traffic control systems whereas cybercrimes such as hacking, phishing, trojan attacks, or denial of service attacks mostly cause temporary disruption or malfunction of private computers which can be repaired and even prevented with appropriate precautionary measures. The legal regime regulating the two phenomena is completely different with cybercrimes being regulated mostly by domestic legal regimes governing cyberspace whereas CNA is regulated by an international legal regime that lays down how wars should be conducted, namely, The Law of Armed Conflict (LOAC) or international humanitarian law. This branch of law is best suited to control the actions of both state and non-state forces during armed conflicts.

Therefore, LOAC will be the main focus of this paper as its application to cyber attacks by non-state actors is analyzed with Part I concentrating on a description of the application of LOAC principles to the use of force in cyberspace. Part II will trace the changes that have occurred in cyber warfare in the 21st century, especially after the 9/11 World Trade Center Attack in the USA emphasizing upon the role of non-state actors engaging in acts of Cyber-Terrorism. Part III will propose the ways in which the law of war can be reconciled with the transition that has taken place in recent times in the manner of carrying out cyber conflicts. This part will also include suggestions as to how other related legal regimes such as customary

international law, international and transnational criminal law can also play a simultaneous role thereby emphasizing on their joint application in the regulation of cyber-terrorism.

Legal Regime Governing Cyber Warfare, Use Of Force On Cyberspace, And The Use Of Internet As A Weapon

Cyber attacks during war are common phenomena in contemporary times and are seldom conducted only as stand-alone operations. It is a manifestation of physical conflict as well as a form of use of force in the virtual world. In terms of legal regulation they are capable of being regulated by two different legal regimes under International Law. One regime discusses the pretext and justifications of resorting to Use of Force and its legality as a form of self-defence against external attacks, namely, *jus ad bellum* rules. The second one imposes restrictions on the means and methods of warfare, namely, *jus in bello* rules which lay down that the means of conducting a war are not unlimited. The manner of application of these rules in the context of CNA needs to be understood before embarking upon the job of tracing the transformation that they need to undergo in keeping with contemporary methods of cyber combat, especially in the post-9/11 era.

Jus Ad Bellum

This body of law governs the legality of resorting to war and using force against an enemy nation and also the exercise of the right of self-defence when facing an attack from opposing forces. The principal international instrument that confers on all states the right to use force both as an aggressor as well as in self-defence is the Charter of the United Nations. It must be mentioned that cyber warfare as a new form of conflict in the modern era has raised severable debatable issues which mainly revolve around the following:

- (i) Do Cyber Attacks amount to Use of Force under Article 2(4) of the United Nations Charter?
- (ii) Do Cyber Attacks reach the level of Armed Attack triggering self-defence measures under Article 51 of the Charter? Can Cyber Attacks be attributed to a State? (Afroditi 2009).

Cyber Attack as a Use of Force

Traditionally when the UN Charter was adopted, it was intended that the term “use of force” will be interpreted in its ordinary sense to mean attacks by the armed forces using kinetic weapons systems and also other coercive measures. This is because Article 31 of the Vienna Convention on the Law of Treaties (VCLT) states that a “*Treaty should be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose*”. A proposal was given at the time of preparation of the Travaux Préparatoires of the Charter that economic coercion should be included as a part of Article 2(4) but that was later rejected in view of Article 31 of VCLT. In keeping with these principles, only the military measures were thought to be signifying the use of force by states under customary international law.

It has to be noted that reconciling the above interpretation of the use of force with the cyber attack phenomenon is a very difficult task. Even though cyber weapons are different from the ordinary kinetic ones used regularly in physical combat, yet the damage inflicted can be of the same proportions (as discussed earlier in the previous section). On the other hand, it can also cause certain types of non-physical damage, i.e. virus and worm attack causing malfunction of software being used in defence networks.

As a result; Prof. Michael N. Schmitt has proposed his own model in order to resolve this issue. He talks about the ‘Consequence-based Approach’ (Schmitt 1999). He proposed that the determinant factors to label cyber attack as a use of force would be important criteria like the severity of the consequences of attack, directness, and accuracy of the attack and the immediacy of the attack. The primary focus of his theory is on the extent of damage caused by a cyber attack which is implied from the severity of the attack. According to his theory then; ordinary hacking of computer networks to gather intelligence information without causing visible physical destruction cannot come within the purview of use of force.

Cyber Attack As An ‘Armed Attack’ To Invite Self-Defence Measures

According to the principles and tenets of international law, any state can resort to self-defence measures if it is facing an armed attack (attack by the military forces through all three routes, i.e. by land, air and sea) launched by another state. In such a scenario, either the state under attack can resort to the use of force as per Article 51 of the UN Charter or the Security Council can intervene to maintain international peace and security under Chapter VII of the Charter.

Article 51 can only be applicable to a cyber attack if such an attack qualifies as an armed attack within the meaning of the provision. Suggestion has been given that for a cyber attack to rise to the level of an armed attack there must be visible physical damage similar to that caused by kinetic weapons. Now, a question arises as to whether self-defence can be used even if damage is yet to be caused and the attack is still ongoing. The answer to this is the use of ‘Anticipatory Self-Defence measures’. For this purpose, a test has been laid down known as the ‘Caroline Case Test’ (Afroditi 2009) which lays down that in order to exercise anticipatory self-defence (Self-defence in anticipation of an attack without even waiting for the first strike from the aggressor which in all likelihood could be a fatal one) a state has to prove that the *“use of the self-defence measures was necessary as the danger was instant, overwhelming, leaving no choice of means and no moment of deliberation”*. Applying this test, a nation launching a cyber attack as an anticipatory self-defence measure might be made aware through an online forum about an impending attack. In turn, that nation may disable the servers of the forum on which the aggressors are used to meeting and discussing their plans of future attacks on states.

Attributing State Responsibility For Cyber Attacks The draft articles on State Responsibility, 2001 prepared by the International Law Commission (United Nations Draft Articles 2001) lay down the rules relating to responsibility of states for the adoption of any unlawful measures. Article 4 of this instrument lays down that *“The conduct of any State organ shall be considered an act of that State under International Law”*. This means that a state organ is always considered to be acting on behalf of its state of affiliation. This rule therefore, is applicable to all acts of use of force by state forces including resort to self-defence measures.

Application of this principle to the cyber warfare context requires tracing of an attack to a unit of a state, i.e. the armed forces, if committed during times of conflict. Tracing an attack to a state will require hiring of experts to track down the attacks through intermediary networks. This is indeed a tough job but if successfully done will result in the application of the Jus in Bello rules as in that case it will tantamount to cyberwarfare during armed conflict involving two or more states.

Jus in Bello (Law of Armed Conflict)

At the end of World War II, these rules were codified into a separate branch of law called International Humanitarian Law consisting of rules regulating the conduct of warfare and procedure for protection of war victims. Cyber attacks during armed conflicts that can be attributed to states are capable of being regulated by this branch of law. Three major principles enshrined in this law are applicable to cyber attacks.

Military Necessity

The necessity of any military attack is the accomplishment of essential military objectives. In pursuance of this, only lawful military targets are allowed to be attacked both in kinetic and cyber warfare. Article 52 of the Additional Protocol I (1977) to the Geneva Conventions defines lawful targets as *“those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage”*.

The risk of launching cyber attacks on defence networks is that very often the attack may be routed indirectly through other systems controlling civilian infrastructure. This can cause heavy collateral damage as well. Thus, for cyber attackers it is very important to identify and directly target defence networks as only such attacks will help the aggressor to gain some military advantage in accordance with Article 52.

Distinction

Articles 48 and 51 of the Additional Protocol require attackers to distinguish between civilian objects and military objectives and also between civilians and combatants and not subject civilians to the dangers arising from military operations. Thus, all attacks should be directed against military objectives only. Applying this to cyber attacks is difficult as often civilian and military networks may be interconnected and are treated as dual-use objects. For instance, an air traffic control system may be controlling both civilian and military flight operations and if damaged would result in civil airplane accidents even though it is simultaneously a military objective as well. Therefore, complying with the principle of distinction requires identification of the nature of use of a particular network especially whether it is predominantly used for military purposes.

Proportionality

It is noteworthy that causing damage to civilian life and property is not completely prohibited as collateral damage can be the result of any war. However, the principle of proportionality requires armies to restrain from destroying civilian life and property in excess of the extent required to gain a military advantage (prohibition of excessive collateral damage). Articles 51 (5) and 57 of Additional Protocol II govern this principle which is applicable even in case of cyber attacks.

Proportionality can be applied quite easily to cyber attacks as the extent of damage caused by such attacks in comparison to kinetic attacks causing physical damage is much less. It is a well accepted fact that cyber attacks minimize collateral damage. However, attacks have to be routed through intermediary civilian networks in such a way that no damage is caused to them. This can be done by cyber experts who can

identify potential targets and avoid other networks which do not have bearing on the war.

The above principles are applicable in all cyber conflicts between states in an international armed conflict. At the same time, they are also applicable to attacks by non-state actors in non-international armed conflicts.

Cyber attacks by Non-State Actors in Non-International Armed Conflicts

The LOAC principles also apply to cyber attacks by non-state actors in non-international armed conflicts which take place between state forces and organized armed groups or between two or more organized armed groups essentially within the borders of one nation. The major issue surrounding cyber attacks by non-state actors is the attribution of such attacks to a state. It is seldom possible to find out whether a non-State organized armed group issuing cyber threats or launching a cyber attack is linked to a state force or not. Even if the source of the attack is traced to a non-state actor, the territorial state will refuse to claim responsibility for the attack and the actions of the non-state group. As per the principles of customary international law, a state should take all measures necessary to ensure that its territory is not used for the perpetration of attacks which will qualify as “Internationally Wrongful Acts”. States need to think about ending the impunity of non-state actors by the simultaneous application of international humanitarian law and their domestic criminal laws if their territory or infrastructure is used to launch such attacks.

At this point it has to be noted that the role of non-state actors in international law has become much more prominent ever since the 9/11 attacks in the US. This incident has brought to the forefront terrorist groups such as Al Qaeda, Taliban, Lashkar-E-Taiyyaba, Indian Mujahideen, HuJi, etc. These groups are characterized by a proper hierarchical structure, a responsible command, trained personnel and a distinct political agenda. These groups are not affiliated to any state or government but at the same time operate on the basis of well connected worldwide networks. Cyber attacks are launched by these groups in order to gather vital intelligence information about potential target states and their defence networks. They may also launch such attacks to cause indiscriminate physical destruction and permanent damage to computer networks. Such acts should therefore be labeled as ‘Cyber-Terrorism’.

The fact that these groups operate individually without any state affiliation has blurred the conventional distinction between international and non-international armed conflicts and has made the application of international humanitarian law on them really tough. It would be safe to say that in the post-9/11 era a new category of armed conflict known as Transnational Armed Conflict (TAC) has emerged thereby requiring a revision of the laws of war and adoption of new mechanisms for its implementation. In this context a detailed analysis needs to be made of this new category. Also the essential changes required in the existing laws will be enumerated and discussed as reconciling the law with the new mode is extremely important. The legal regimes that need to be studied for the purpose of application to cyber-terrorism are customary international law, international criminal law, and transnational criminal law. The first one is important as it is expected to give to the international community a comprehensive definition of the term ‘terrorism’. The other two are required for the imposition of sanctions on terrorist acts. However, changes are required to be made to these laws in order to recognize all forms of terrorism.

Customary International Law

The international community has been grappling with the idea of adopting a single, all-pervasive treaty-based definition of the term terrorism since 1937 when the then predecessor of the United Nations, i.e. the League of Nations was in existence (Saul 2010). The objective of this paper is not to analyze in detail all those historical efforts but to suggest that if and when a definition is indeed formulated, cyber-terrorism should be incorporated as one of its constituent elements. At the moment, there is not international instrument that defines and criminalizes all forms of terrorism.

Transnational Criminal Law

This branch of law mainly revolves around the United Nations Convention on Transnational Organized Crime (UNTOC) signed in 2000 in Palermo, Italy. It defines crimes like drug trafficking, money laundering, human trafficking, etc which are committed globally and urges the member states to co-operate in order to effect the arrest, trial, and punishment of those involved in the perpetration of these crimes using their respective domestic legal regimes. This treaty was adopted specifically to address crimes committed by organized criminal groups, i.e. mafia gangs and terrorist organizations operating through global networks.

One drawback noticed in this law is its silence on the aspect of criminalizing and punishing terrorism in all its forms. One possible reason could be the absence of a well-accepted working treaty definition at the international level which needs to become a part of customary international law.

After the adoption of a treaty-based definition, terrorism in all forms should be made a part of the UNTOC. This step would ensure that terrorism, especially cyber-terrorism is recognized as a transnational organized crime. The primary logic behind this is that terrorism in contemporary times has become a transnational crime with international effects just like the other transnational crimes already a part of the UNTOC.

International Criminal Law

Ever since the adoption of the Statute of the International Criminal Court at Rome, Italy in 1998 a new branch of law called international criminal law has emerged. This law has established a permanent International Criminal Court (ICC) at The Hague, Netherlands and punishes individuals for core international crimes committed mostly during armed conflict which threaten international peace and security. Signatories to the statute have formed a group called 'Assembly of States Parties (ASP)'.

It was deliberated at the time of adoption of the statute that transnational organized crimes (hailed as treaty crimes) including terrorism should be included in the statute but that suggestion was later rejected due to the absence of an international definition of terrorism. It was also felt that transnational crimes are not heinous enough to be tried by a permanent international body.

Terrorism including its financing has been condemned by the International community. Therefore, the condemnation of cyber-terrorism as well naturally follows from the general condemnation. Thus, it is now submitted that terrorism including cyber-terrorism should be adopted as a separate provision in the Rome Statute under "Transnational Organized Crimes". This should also include other treaty crimes like drug trafficking, money laundering etc. Transnational crimes are putting international borders and security in jeopardy and have assumed serious proportions in the 21st century.

Need For Reforms In International Law In Accordance With LOAC

The 9/11 incident in the USA prompted the then US President George W. Bush to declare a “Global War on Terror” against the terrorist organizations. Subsequently, attacks were mounted by US Armed Forces to completely wipe out terrorist groups like Al Qaeda and Taliban which had a major role to play in the planning and perpetration of 9/11. This gave rise to armed conflicts between these dissident armed groups and government forces (especially the U.S. forces) which were not confined within the borders of one nation. Since then more terrorist groups based in different countries have attacked and engaged in conflict with other states. These armed conflicts cannot be labeled as “international armed conflicts” due to the involvement of non-state organized armed groups (OAGs) nor can they be identified as non-international armed conflicts as they are cross-border in nature and not just confined within the borders of one nation.

Therefore, the important issues that arise in relation to such conflicts are:

- (i) Is there a need to add a third category of armed conflicts to the laws of war and if so what name can be given to these conflicts?
- (ii) Whether cyber attacks launched during these conflicts amount to armed attack inviting self-defence measures?
- (iii) How will the Jus in Bello rules apply to cyber attacks during these conflicts?
- (iv) Do other laws need to compliment the LOAC to successfully criminalize such attacks and make them punishable? All these questions need to be answered in great detail.

The word ‘Transnational’ means transcending national boundaries or across the borders of several nations and applying this meaning to the non-state armed groups would imply that the groups are mostly based within the borders of one nation but execute their plans across the borders of several nations. Thus, their location is internal but operation is transnational thereby threatening international peace and security. Subsequently, if and when states retaliate against these groups, the conflict that ensues can be termed as a transnational armed conflict (TAC).

Some scholars have already put forward certain academic arguments in favor transnational armed conflict without going into the question whether this new category should be included in the law of war. They have also said that the time is not yet ripe to make immediate changes to the laws of war and the existing LOAC principles themselves can be applied to this new category (Corn and Talbot 2009)[2]. The principal argument put forward by the scholars for saying so is that transnational armed conflict is not a new concept and has been existing ever since the emergence of IHL. They have identified it as a manifestation of a mere non-international armed conflict.

However, it is high time for steps to be taken to formulate new mechanisms for application of international humanitarian law to these conflicts. In the past few years after 9/11, the incidents of terrorism have crossed national boundaries as terrorist groups have perpetrated large scale attacks which have been carried out over a certain period characterized by systematic, continuous, and planned use of armed force. Moreover,

constant threats of use of force have been issued by terrorist groups using the electronic and print media prompting governments to adopt anticipatory self-defence measures.

The application of the *jus ad bellum* rules will remain the same while the major transformation needs to come in the *jus in bello* rules embodying the laws of war. The possibility of introducing a Third Protocol to the Geneva Conventions needs to gather momentum now as this is the need of the hour.

Jus Ad Bellum and Jus in Bello perspectives

The nature of cyber attacks launched by terrorist groups is different from ordinary cybercrimes. The people responsible for heading and commanding terrorist groups provide extensive training of skills to ordinary individuals to transform them into experts specializing in various aspects of a battle. This includes training to gain expertise in computer network operations or hiring cyber networking experts to carry out Information operations (IO). Thus, the experts' use of computer networks to launch attacks makes the computer system a weapon or arms for attack. Apart from that, the large scale physical damage caused would tend to set a high threshold of consequences thereby qualifying the entire operation as an armed attack. It is submitted that these attacks should always qualify as acts of cyber-terrorism as the ultimate object is to create terror in the minds of people and their governments.

Obviously, on facing the threat of cyber-terrorism it would be perfectly legal for the affected state to take self-defence measures against the terrorist groups. As per the principles of customary international law embodied in the United Nations Charter, this would justify the resort to use of force by states in response to an armed attack according to Article 51 of the Charter which in turn satisfies the *jus ad bellum* aspects of the law of war.

The most important aspect though is considering the nature of attacks in the context of TAC how would international humanitarian law (containing the *jus in bello* rules) be applied to the use of force by states and secondly the attacks launched by the terrorist groups.

Jus in Bello, Cyber-Terrorism and States' Response

The global war on terror initiated by the U.S. and supported by major players across the globe has meant that governments now have a tendency to invoke the principles of LOAC to justify actions taken in self-defence against terror groups. This seems to follow naturally as the retaliation against terror in essence is a war or an armed conflict. Therefore, it needs to be seen in what manner the basic principles of international humanitarian law apply to acts of cyber-terrorism.

Military Necessity

Countries involved in the war on terror have always successfully stated that non-state armed groups challenge the defence establishments of various countries and retaliating against them through the use of armed force is therefore a military necessity. The same concept will apply in case of cyber-terrorism as well which easily justifies attacks against the terrorist groups using the state defence networks. Terror groups can cause unnecessary and unending physical damage to civilian lives and property through attacks launched in cyberspace which is a direct violation of LOAC principles and therefore there launching

retaliatory attacks to thwart those attempts is an essential military objective within the purview of Article 52 of the First Additional Protocol. Moreover, they might attempt to gather vital information about the civilian and military infrastructures by hacking into defence networks against which states can take precautionary and preventive measures as well. This is again a valid military objective.

Principles of Targeting (Distinction and Proportionality)

When defence forces launch cyber attacks against networks used by terror groups, it is extremely important that they keep in mind that no unnecessary damage is caused to other civilian or defence networks through which data travels to reach the systems being used by terror groups. Thus as per Articles 48, 51(5) and 57 of the First Additional Protocol, no loss of civilian life and property should be caused through the counter-attacks. This requires handing over the responsibility of network operations to cyber experts who can identify the target terrorist networks directly and can also use techniques to avoid causing damage to intermediate networks. There may be armed forces personnel who are specifically assigned this task. On the other hand, if civilian experts are hired they will lose all protection guaranteed by the LOAC principles and will transform into “Civilians taking direct part in hostilities”. In case of violation of these principles the members of the state forces and those in command can be attributed with Individual Criminal Responsibility and Superior Responsibility for Grave Breaches of the Geneva Conventions. They will thus be liable for the commission of war crimes in Non-International Armed Conflict[6]. A tendency might arise to justify all actions as self-defence measures in the war on terror but state actors exercising authority always have the obligation to follow the Rules of Engagement (ROE).

Application of *Jus in Bello* Principles To Terrorist Groups In Transnational Armed Conflicts

After a careful study of scholarly opinion, till date on this issue it has to be said that all previous arguments are outdated and outmoded by the fact that identifying the acts of terrorist groups as grave breaches of the Geneva Conventions and subsequent criminalization of such conduct is the need of the hour. There is no denying the fact that by now transnational armed conflict has indeed become a third dimension of international humanitarian law.

As a result, the international community especially the ‘High Contracting Parties’ to the Geneva Conventions need to realize that the time has come to add another Additional Protocol III to the Geneva Conventions to regulate the conduct of warfare in transnational armed conflicts. The rules of this protocol should be drafted in such a way so as to be applicable to acts of cyber-terrorism just like the other two protocols.

TAC As An Armed Conflict Incorporating The War On Terror

It needs to be defined as “An armed conflict between the armed forces of a state and Dissident Organized Armed Forces not belonging to any state operating beyond the borders of one nation”. This will ensure that transnational conflicts between state and non-state terror groups are recognized as an armed conflict in consonance with the ongoing war on terror.

Combatant Status

The terrorist groups satisfy the eligibility criteria to be conferred the status of lawful combatants but unlike state forces they are under no obligations to follow the principles of distinction and proportionality. Earlier, under the Second Additional Protocol, non-state actors captured by enemy forces during non-international armed conflicts were not given any definite legal status unlike the Prisoner-of-War (POW) status accorded to detainees of international armed conflicts. Non-state actors have so far been treated as ordinary detainees.

However, detainees of transnational armed conflicts should be governed by the Third Geneva Conventions relating to treatment of POW's as this category is constituted by the war on terror and other similar conflicts in the nature of wars between state and non-state transnational groups. This will put states under an obligation to grant POW's status to all lawful combatants belonging to non-state armed groups affording them the basic guarantees.

At the same time, this will encourage non-state groups to reciprocate and they will be obliged to a certain extent to afford protection and fundamental guarantees to members of state forces captured by them[7].

A separate provision therefore needs to be made in the newly proposed protocol to extend the application of Third Geneva Conventions to transnational conflicts.

Distinction and Proportionality

The legal recognition of transnational conflicts as war means that both parties are obliged to follow these rules. In case of violation, perpetrators would be punishable for the commission of war crimes under the Rome Statute of the International Criminal Court.

Cyber-terrorism in transnational armed conflicts can be governed through the new protocol with the above rules applying to them. However, only the application of the above principles will not be enough as there is again a need to criminalize the actions of terrorist groups for a much more effective implementation of international humanitarian law. For this purpose, the need of the hour is the simultaneous application of those laws that are required for defining and criminalizing terrorist acts in conjunction with the law of war.

Nature Of Armed Conflicts And Cyber Warfare After 9/11

All these discussions show that in order to combat cyber-terrorism only the LOAC principles are not enough. The High Contracting Parties to the Geneva Conventions and the ICC Statute need to think about adding a third protocol and transnational organized crimes to the respective body of laws. Apart from that, respect has to be generated for the law of war by its strict enforcement especially against the non-state groups even if such groups only threaten to use force. Particularly in case of cyber-terrorism; states need to hire experts to trace the location of the attackers and bring them before international criminal courts and tribunals for trial. Cyber attackers use sophisticated technology which is evolving every day and therefore it is important for states also to constantly upgrade their technology as well especially the technical equipments being used by the respective defence departments.

Conclusion

Books

(1) Prof. Saul, B 2010, *Defining Terrorism in International Law*, Oxford University Press, New York

Articles

(1) Schmitt, MN 1999, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, *Columbia Journal of Transnational Law*, Vol. 37

(2) Corn, G and Talbot, E 2009 'Transnational Armed Conflict: A Principled Approach to the Regulation of Counter-Terror Combat Operations', *Israel Law Review*, Vol. 42, No. 46

Internet Sources

(1) Milanovic, M and Vidanovic, V., H 2010 'A Taxonomy of Armed Conflict' Viewed 7 September, 2014

(2) 2001 Draft Articles on the Responsibility of States for Internationally Wrongful Acts, 2001 UN Doc. A/CN.4/L.602/Rev. 1 Viewed 7 September, 2014

(3) Jennings 1938 The Caroline and Mcleod Cases, *American Journal of International Law*, Vol.32, Page 82 in Afroditi, P 2009 'Application of International Law in Cyber Warfare Operations', Viewed 7 January, 2013,